The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.



U.S. AND COALITION COMMAND AND CONTROL INTEROPERABILITY FOR THE FUTURE

BY

LIEUTENANT COLONEL WILLIAM R. POPE United States Army

DISTRIBUTION STATEMENT A:

Approved for Public Release. Distribution is Unlimited.

USAWC CLASS OF 2001



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20010605 200

USAWC STRATEGY RESEARCH PROJECT

U.S. and Coalition Command and Control Interoperability for the Future

by

Lieutenant Colonel William R. Pope U.S. Army

Colonel James Thomas Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College Carlisle Barracks, Pennsylvania 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ii

ABSTRACT

AUTHOR:

Lieutenant Colonel William R. Pope

TITLE: U.S. and Coalition Command and Control Interoperability for the Future

FORMAT:

Strategy Research Project

DATE:

01 April 2001

PAGES: 35

CLASSIFICATION: Unclassified

The U.S. Army is on a course to transform its forces with capabilities that are generations beyond those in existence today. These same forces are also more likely than ever before to serve in nearly all forms of future operations with forces from other nations. Will the Army's transformation enhance its ability to interoperate with allied and coalition partners or will it broaden a gap that already exists?

Interoperability among our U.S. Services is a challenge, but is becoming less of an obstacle as the Joint community strengthens our resolve to comply with joint interoperability standards. Interoperability with coalition partners is improving in some regards and is becoming more difficult in others. The bi-polar nature of this situation has the potential to expand if steps are not taken to codify our intentions with coalition partners and work toward solutions that enable mutually supportive relationships.

The Army faces the challenge to develop future systems capable of supporting the exchange of Command and Control (C2) information needed to support our operations and those of our allies. Sufficient knowledge exists in the Command, Control, Communications, Computers, and Intelligence (C4I) community to recognize the importance of coalition interoperability, but little detail exists to determine the actual information or knowledge transfer that needs. This paper will explore the needs of U.S. and coalition partners in the exchange of C2 information.

iv

TABLE OF CONTENTS

ABS	STRACT	!!!
ACI	KNOWLEDGEMENTS	VII
U.S	. AND COALITION COMMAND AND CONTROL INTEROPERABILITY FOR THE FUTURE	1
	WHO WILL BE INVOLVED IN FUTURE DEPLOYMENTS?	1
	JOINT FORCES	1
	MULTINATIONAL FORCES	1
	ASYMETRIC THREATS	3
	WHAT DO WE NEED TO SHARE?	3
	COMMAND AND CONTROL	3
	MULTINATIONAL COMMAND AND CONTROL	3
	INFORMATION RELEASEABILITY	5
	HOW DO WE SHARE THE NECESSARY INFORMATION?	6
	LANGUAGE	6
	INTEROPERABILITY	7
	REQUIREMENTS FOR SUCCESS	8
	Voice	8
	Facsimile	8
	Electronic Mail	9
	Defense Messaging System	9
	Relevant Common Operational Picture	10
	Collaborative Planning	11

	INFORMATION SUPERIORITY	. 12
	TRANSFORMATION	.12
	US PACIFIC COMMAND (PACOM) EXPERIENCES	15
	RECOMMENDATIONS	16
	POLICY	17
	TECHNOLOGY	
	STRATEGIC VISION	18
	CONCLUSION	19
ENDNOTES		.21
BIBL	BIBLIOGRAPHY	

ACKNOWLEDGEMENTS

I would like to thank the many allies I have worked with in the past, who provided me with the professional inspiration to write on this topic, Mr. John Crooks, of Delphin Systems, and Mr. George McVeigh of the Joint Staff J6, who assisted me in my research.

U.S. AND COALITION COMMAND AND CONTROL INTEROPERABILITY FOR THE FUTURE

Over the course of the last 100 years the United States has grown from an isolated western-hemisphere power, to one increasingly involved in world affairs. Today the US is widely accepted as the world's sole global superpower. In the words of former president William Jefferson Clinton, America has become the world's "indispensable nation." To maintain such a position in the world without draining our resources we must enlist the cooperation of our allies at every opportunity. When and wherever we engage with allies we must show our leadership by fielding interoperable communications equipment that is capable of efficiently and effectively sharing the Command and Control information necessary for coalitions to succeed.

Assessing the needs for interoperability between the US and other nations is a daunting task to say the least. Policy will determine who we share information with, but the US Army's transformation will determine the extent to which the permitted information can be exchanged over the new technologies of advancing telecommunications. This paper will explore the nation's needs for military interoperability and will assess the Army's ability to meet those needs with the capabilities being developed through the transformation process.

WHO WILL BE INVOLVED IN FUTURE DEPLOYMENTS?

JOINT FORCES

Strategic and operational planners from across the US military anticipate that practically all future deployments of US forces will comprise more than one Service. Some situations may require the capabilities of only one Service, but in most cases we will employ a joint force comprised of both Active and Reserve Components.² The integration of core competencies provided by the individual Services is essential to the joint team, and the employment of the capabilities of the Total Force (active, reserve, guard, and civilian members) increases the options for the commander and complicates the choices of our opponents.³ Our commitments require multi-mission capable US forces; interoperable among all elements of US Services and selected foreign militaries; with the capability to coordinate operations with other agencies of government, and some civil institutions.⁴ The joint force, because of its flexibility and responsiveness, will remain the key to operational success in the future.

MULTINATIONAL FORCES

Each situation that our nation faces will dictate the extent to which other friendly nations contribute forces. The joint force of the future will achieve its goals through full spectrum dominance - the ability of US forces, operating unilaterally or in combination with multinational

and interagency partners, to defeat any adversary and control any situation across the full range of military operations.⁵ In addition to the participation of multinational military forces, we must be prepared to make optimum use of the skills and resources provided by regional and international organizations, non-governmental organizations, and private voluntary organizations when possible. The challenges in dealing with these non-US or non-Department of Defense (DOD) organizations require as much, and in some cases more, detailed planning and cooperation than when dealing with other nations' military forces.

Geographic CINCs strive to establish the best relations possible with every nation-state in their regions. CINCs wish to exercise with most of these nations to get to know them better and to help them get to know the US better. As the US looks toward its role as a global leader there are countless possible scenarios that could place US servicemen and women in operations with forces from other nations. While the preponderance of our most recent operations have been peace support operations, there will continue to be a need to be able to fight alongside other nations in major theaters of war. Our US armed forces will continue to support government policies and politics, our diplomatic and economic elements of leadership, treaties and alliances in an international environment for the foreseeable future.

The U.S. military plays a crucial role in shaping the international security environment in ways that protect and promote U.S. interests. Through overseas presence and peacetime engagement activities such as defense cooperation, security assistance, and training and exercises with allies and friends, our Armed Forces help to deter aggression and coercion, build coalitions, promote regional stability and serve as role models for militaries in emerging democracies. Engagement activities, including information sharing and contacts between our military and the armed forces of other nations, promote trust and confidence and encourage measures that increase our security and that of our allies, partners, and friends.

Multinational operations, both those that include combat and those that do not, are conducted within the structure of an alliance or coalition. An alliance is a result of formal agreements between two or more nations for broad, long-term objectives. A coalition is an ad hoc arrangement between two or more nations for common action. We are successfully adapting our military alliances to new realities and building security relationships with new coalition partners.

The support and participation of allies, friendly nations, and relevant international institutions will be considered in the decision to use US military forces. When our vital interests are at stake, we are prepared to act alone. But in most situations, working with other nations increases the effectiveness of each nation's actions and lessens everyone's burden.¹⁰

ASYMETRIC THREATS

In peace operations, as in war, we must be aware of all the possible threats that could endanger multi-national cooperation. A number of "wild card" threats could emerge to put US interests at risk. Such threats range from the emergence of new technologies that neutralize some of our military capabilities, to the loss of key allies or alliances. Because of the global nature of (unclassified) information networks, no area of adversarial activity has greater international implications than high technology crime. Adversaries are not hampered by international boundaries, since information can be transmitted quickly and covertly via telephone and information systems. Many of the challenges are extremely difficult to address without international consensus and cooperation. We seek to develop and implement new agreements and encourage cooperative research and development with other nations to address these challenges. 12

WHAT DO WE NEED TO SHARE?

COMMAND AND CONTROL

Success on the battlefield or in operations other than war requires effective command of the forces that are involved in the operation and control of the operations that the forces are commanded to undertake. Joint Publication 3-0, <u>Doctrine for Joint Operations</u>, defines Command and Control (C2) as "... the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission." Command at all levels is the art of motivating and directing people and organizations into action to accomplish missions. Control is inherent in command. To control is to regulate forces and functions to execute the commander's intent. Control permits commanders to acquire and develop specific instructions from general guidance. Ultimately, it provides commanders a means to measure, report, and correct performance.¹⁴

MULTINATIONAL COMMAND AND CONTROL

Military operations in regional crises may often involve coalitions different from familiar, long-standing alliance structures. Command and control in multinational contingency operations is particularly critical. No single command structure best fits the needs of all alliances and coalitions. Each coalition or alliance will create the structure that will best meet the needs, political realities, constraints, and objectives of the participating nations. Under no circumstances will the President ever relinquish his constitutional command authority over U.S. forces, but there may be times in the future, just as in the past, when it is in our interest to place

U.S. forces under the temporary operational control of a competent allied or United Nations commander. 17

Alliance command and control arrangements are likely to be predetermined, or negotiated within a treaty of the alliance long before forces are even engaged in an operation. Coalition command and control arrangements will not be established until the coalition is established. United States combatant commanders and subordinate Joint Force Commanders are also likely to operate with agencies representing other US instruments of national power, with foreign government, and with non-governmental and international organizations in a variety of circumstances.¹⁸

The conditions under which a military leader commands, controls, or supports apportioned forces dictate the constructs of interaction that will be necessary between senior and subordinate units. The basic constructs are Combatant Command, Operational Control, Tactical Control, and support.

Combatant Command (COCOM) is, by definition, restricted to US forces under title 10, US Code, or is as directed by the President of the United States in the Unified Command Plan. COCOM, as it is defined in the US, does not apply to forces from other nations under the direction of a US commander. Because governments will almost never surrender sovereignty and aspects of command, such as force structure, promotion, and discipline, commanders in peace operations seldom have genuine COCOM over forces not from their own nation. ¹⁹

Operational Control (OPCON) is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. One could think of this as the equivalent of long-term leasing. The Clinton Administration policy on reforming multilateral peace operations embodied in Presidential Decision Directive 25 (PDD-25) indicates that the US President will, "on a case by case basis consider placing appropriate US forces under the operational control of a component UN commander to achieve specific military objectives. Allied forces could be placed under the OPCON of a US commander, and as described above, in very limited circumstances US forces could be placed under the OPCON of an allied commander.

Tactical control could be considered equivalent to a short-term rental. Tactical Control (TACON) is the authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and usually local direction and control of movements or maneuvers necessary to accomplish assigned missions or tasks.²² The support of forces placed upon TACON is the responsibility of the parent unit of the unit

placed under TACON. The supported commander is allowed to use the TACON forces without the burden of supporting them, but also knows that they may be reassigned at any time.

Support is a function, established by command authority, where one unit provides aid, protection, complements, or sustains another unit or force. General support and direct support are two forms of this type of command relationship.

The conditions that cover forces apportioned to a command, and the constructs of interaction between senior and subordinate units, become more complex when the units within the command come from different nations. The information that enables interaction is useless unless it is shared. In order the share information the US must first determine if it is releasable to other nations.

INFORMATION RELEASEABILITY

"Information" is defined as facts, data, or instructions in any medium or form.²³ The military use of information can be applied in different ways for different purposes. It may consist of intelligence, logistics, plans, capabilities, activities, objectives, command directives, or orders. The value of information may change in relation to the objectives during peace, crisis, conflict, or post-conflict, as well as during the various phases of an operation.²⁴ Information itself can be a strategic resource vital to success at any level of operation.

The U.S. is typically more selective about the information that it shares with other nations than it is about the nations that it participates in exercises with. There are formal bonds of trust with the most trusted nations. Many of these nations have compatible technological capabilities that would enable interoperability. Some of these nations subscribe to the same technical standards that we do, while others in this group do not. Any nations that we consider as potential peers in this group have the economic capacity to keep pace with us. Other nations desire to work with us, to learn from us, to be mutually supportive, but do not have the economic resources to do so. Some nations desire what we have, to improve their own capabilities, but are less likely to be mutually supportive in War or Operations Other Than War.

Should the US share more information with some allies than with others? This is a question that is left for the National Command Authority, with the advice of the Departments of State, Defense, and others. The answer to this question, and our first reality when dealing with allies, is that our diplomatic and foreign relations between the US and every nation-state in existence change with the frequency of the winds. The types of information that we are able to share, the classifications of that information, and the latent risks inherent with sharing our information are fluid and ever changing.

The second reality that we must face is that there is no nation that the US will ever share all its classified information with. As close as our Canadian and British allies are in common interests and objectives, there will always be limits to sharing the most highly classified information with these nations.

The third reality is that regardless of our relationships with other nations, we will be faced with situations where we must share information with a nation or nations that we do not entrust with our classified information. In order to work together we will need to communicate, even if it does not include the communication of classified information.

HOW DO WE SHARE THE NECESSARY INFORMATION?

The necessity of information is relative to the operation that it supports. While US policy sets the standards for releasability of classified information, determining which information needs to be shared is ultimately the responsibility of the operational commander. As we look to the future systems being developed under the Army Transformation to open avenues of interoperability that a future commander will need, it is worthwhile to consider a few basic components of information exchange.

LANGUAGE

In order for information exchange to take place, the information must be understood by the transmitting and receiving parties. The oldest and most fundamental challenge to interoperability is language. At every level of multinational training and operations common procedures are useful and necessary, but they are incredibly difficult to manage without effective information communication between the various elements. Language is the first barrier that must be overcome and is the first step toward interoperability.

In the political and diplomatic environment of the European Union English has been selected as the preferred language. The same considerations have been applied at the United Nations and NATO. Broadcast media has been moving toward English as was signaled by the British Broadcasting Corporation's discontinuance of programming in German in March of 1999. BBC research showed that a large number of German decision-makers listen to the World Service in English. The Frankfurter Allgemeine Zeitung newspaper reported 'We all now speak English well enough.' Technical disciplines have also found the need for standardization in order to achieve interoperability. Among the most notable is the use of the English language throughout much of the world's air traffic control operations.

One solution to interoperability would be for all participating nations agree to use a single language, such as English. This could provide a common reference that all would be expected

to use. However, this puts a burden upon non-English speaking nations to teach leaders, translators and interpreters the language.

A second, and more accommodating approach would be to take advantage of evolving technology. Advancements in software applications for written language translation have made it possible for a document to be created and then viewed in dozens of different languages. This would work at the operational and strategic levels as national militaries are becoming more comfortable with the use of Internet based applications to share information. It is also now possible to use translation software to enable a computer user accessing a network to select the language that is to be viewed and software that translates the content of the web page into that language.

One US Pacific Command (PACOM) interoperability initiative has engendered greater military-to-military cooperation throughout the region, using an Internet web site. Asia-Pacific armed forces post information that is of general interest to the other military forces in the area on this web site. ²⁶ In an interview with Armed Forces Journal, the US PACOM Commander in Chief (CINCPAC) endorsed such capabilities. He said "We are finding new uses for it all the time, but fundamentally, it's a way for us to communicate with all military organizations in the Asia-Pacific region." Such technology may have applicability to command and control software, as well as to web page translation, and may be useful at the tactical level. The use of internet capabilities on the battlefield to distribute and share information has a great deal of promise and is a component of the Army's Transformation effort that will be described later in this paper.

While the standard procedures for using multi-language capable web sites are not precisely defined, they are worthy of continued support to enable partner nations to better understand each other. Any expansion of technical capabilities such as these will come at a financial cost, and the cost-effectiveness will have to be determined by the utility of the translation services provided, both to the US and to other nations. The training of language specialists and the procurement of language translation capabilities should be continued while we strive for more seamless exchange of information between the US and our allies.

INTEROPERABILITY

Interoperability is the foundation of effective joint, multinational, and interagency operations.²⁸ Our military must be ready to fight as a coherent joint force -- fully interoperable and seamlessly integrated.²⁹ We also must work with Allies and coalition partners to help

improve their interoperability with our forces, in order to bolster the effectiveness of multinational operations across the full spectrum of potential military missions.³⁰

Interoperability is defined in Joint Pub 1-02 as "the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together." Interoperability includes common logistics items and information sharing, in addition to communications interoperability. Beyond the embedded technologies and adaptive organizational structures that will be needed in the future, interoperability in the past, present, and future requires compatible processes and procedures to engage in collaborative planning, and adapt as necessary to situations as the develop. These features are not only vital to the joint force, but to multinational and international operations as well. 32

REQUIREMENTS FOR SUCCESS

The means that we use to communicate are often the keys to determining the speed and, more importantly, the effectiveness of the information exchange. By looking at various means of communication, we can determine the criticality of the interoperability needed for successful information exchange with our allies.

Voice

Voice communications remain a key ingredient to tactical and operational command and control. Differing languages within a Multi-National Force can present a real challenge to unity of effort. At the purely tactical level of conventional operation there have been fewer times when multinational forces, speaking different languages, needed to operate as an intermixed force than at the operational or strategic levels. This is changing as US forces interact with forces from other nations to support operations other than war or peace operations. On a non-contiguous field of operation it is possible that different nations will have different sectors that could be interwoven. In these conditions, the human voice and language is critical to understanding any mission, especially in times of conflict.

Facsimile

Facsimile traffic between elements of a coalition has transitioned from the written word to graphics. The need to write out a message and fax it to a counterpart in order for it to be translated has given way to the telephone, email, and data communications. The traffic that is still carried by facsimile machines contains graphics of the area of operation, friendly and enemy

situations, etc. Until we have effective communications of graphics between nations over data transmission means the facsimile will continue to be used over voice circuits to carry graphics.

Electronic Mail

The less formal and less secure means of message communication is via commercial electronic mail. This form of communication is fine in environments where the supporting network or networks are used for traffic that is consistently and completely of only one classification level, such as unclassified or SECRET. Since most electronic mail is not encrypted, the network that carries the traffic must be secured to the highest level of traffic that it carries. While this may sound simple, it is historically prone to compromise by users unintentionally exceeding the classification levels of the network. With the expanding use of Public Key Encryption the security of unclassified email can achieve a level of trust in a coalition environment that could be utilized to exchange sensitive but unclassified information.

Dedicated secure communication networks that interconnect all allies with access to classified information to a certain level, such as CONFIDENTIAL, would otherwise be necessary. Such networks then require the use of interoperable communications security (COMSEC) equipment and the distribution of cryptographic materials to enable the COMSEC equipment to exchange traffic with similarly configured equipment. Both the COMSEC and the cryptographic materials are strictly controlled by DoD policy (DoD 5200-1R), and authorizations for distribution to allies varies depending upon the nations requesting this sort of support.

Defense Messaging System

Electronic mail has effectively replaced record formal message traffic and courier service on the modern battlefield. The US Defense Message System (DMS) is the more formal means of electronic mail allowing varying levels of classification. Sender and receiver can be verified with electronic signatures, and the message that is included in the mail can be certified as being complete and un-compromised.³⁴

The use of this system in a coalition environment would simplify the distribution of message traffic between users with differing levels of access to classified traffic. In the DMS system, a user's security access is known by the system through the use of electronic certificates of authenticity and Personal Computer Memory Card International Association (PCMCIA) cards. These DMS certificates bind a unique name to the keys used for cryptography. DMS currently relies on the use of PCMCIA cards that provide the cryptographic services. Traffic that is above that user's security access level will not be delivered to that user. The variable output of DMS messages to conform with internationally

recognized Joint Army, Navy, and Air Force Publication (JANAP) formats would simplify the exchange between US and allied message handling systems. Multi-functional interpreters that are able to translate between DMS, JANAP and other message formats could also be used.

The primary challenges to fielding this capability to allies come in the form of network accessibility and interconnectivity. The majority of US DMS users are interconnected via a US network called the Secret Internet Protocol Router Network (SIPRNET). US Department of Defense policy precludes allied direct connections to this network, and only in the most regulated settings are allied networks allowed to connect to the SIPRNET via security gateways, such as the DMS High Assurance Guard. The Guard (sometimes referred to as the "Defense Information Infrastructure (DII) Guard") provides secure guard services between security domains (e.g., Secret and Unclassified).³⁷

A secondary area of concern for allied use of DMS revolves around the willingness of the US Government to release DMS technologies to allies. While individual users or organizations could be certified for use on a case by case basis, permission to create certificates, and authentication of allied users without the direct supervision of the US government could be drawn into question. Steps are being taken currently by the Assistant to the Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) to review what policies and procedures would be necessary to enable allies with these capabilities.

Relevant Common Operational Picture

The need for real-time knowledge of where friendly and enemy troops, ships, and aircraft are at any given moment is more of a necessity on the asymmetric battlefield today than ever before. The use of maps with acetate overlays, grease pencils, and map symbols continues to be prevalent, predominantly in environments where common communications networks can not be shared, such as in a restrictive coalition environment. The breakdown of communications is in some cases by design, and in other cases due to technical incompatibles. The voids established by design are predominantly due to policy regulations precluding the sharing of certain types or classifications of information between the US and other nations. The voids in technical interoperability include differences in telecommunications standards and in software application compatibility. It would be optimal for US and allied ground component commanders to share relevant common operational information, but these voids are prohibitive. Overcoming or bypassing these voids requires the commanders to generate, staff, and forward for approval some form of a request for exception to policy, or to direct a method of technological first aid, or both.

The digitization of unit designations, and symbols, along with the classification of the information that denotes the location of those units is becoming more common. The application, which enables users to view this information from anywhere on a common network, has become known as a Common Operational Picture (COP). US and coalition partners, including the UK, Australia, Canada, and NATO nations, have successfully shared and contributed to a form of Common Operational Picture during Joint Staff sponsored Joint Warrior Interoperability Demonstrations (JWIDs) since 1996. During these demonstrations Allies are interconnected over a common Coalition Wide Area Network (CWAN), which operates at the coalition-releasable SECRET level, and is separated from US Secret networks by highly protective firewalls and gateways. In this configuration the allies are able to view the locations of units who's positions are classified coalition-releasable SECRET or below, but are unable to see the locations of units whose positions are more highly classified.

The Common Operational Picture is a capability that can improve coalition command and control, but there are second order effects to the widespread distribution of COP data. As more and more information is digitized and unit information is relayed, the common operational picture has a tendency to become cluttered. The reduction of the fog that this clutter can create and the presentation of a common operational picture that is 'relevant' to the area of interest of each land, sea, or air commander must be continued. A coalition shared relevant common operational picture will invariably improve our effectiveness on the battlefield and may save lives as well.

Collaborative Planning

The planning of any coalition operation is ultimately the responsibility of the nation that leads the coalition. The success of the coalition hinges upon the identification of each nation's needs and capabilities. When communications networks are segmented and divided between those allies can and can not use the planning process is hampered. Joint Pub 3-16 states that: Staffs should evaluate the level of standardization and interoperability among participating nations and, where situations permit, come to agreement on which nations will be responsible for support and the procedures and methods to be used. Collaborative planning tools available today can offer interactive planning, coupled with Video Teleconferencing Capabilities (VTC), but all the users must be on the same level of classification of network, and have access to the information on that network.

The US Army Battle Command Battle Laboratory (BCBL) at Ft. Leavenworth is leading an effort to bring collaborative coalition planning together in the Simulation and C2 Information

Systems Connectivity Experiments (SINCE). The objective of the SINCE Program is to define, implement, experiment and demonstrate the feasibility of interfacing and networking emerging Brigade/Battalion C2 systems and appropriate modeling and simulation systems/capabilities into an integrated coalition force collaborative planning environment. Experiments such as these will help guide the formation of command and control concepts for the transformation of the Army so that the objective force may enjoy information superiority. Coalition networks based upon the findings of programs such as SINCE should become the standard for future US operations rather than the exception of the rare experiment.

INFORMATION SUPERIORITY

Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting or denying an adversary's ability to do the same. ⁴⁰ In a coalition operation is it necessary for the entire coalition to have information superiority? The instinctive answer is that the US is the only nation that needs, or for that matter is capable of achieving, information superiority. The fact is that the coalition must maintain the tenants of information superiority even if one nation remains the strongest and most capable of all the nations. The coalition must be able to protect it's own information, must understand the adversaries capabilities, and be able to influence the adversary to do the coalition's will. Not all nations must possess all these capabilities, but at a minimum they must all be able to protect the information that they posses and share. As interoperability expands and information distribution becomes more fluid the need for information security expands with it. The coalition must have information superiority over its adversaries.

Consideration should be given to possible degradation of communications due to extended distances over which a multi-national force must operate and the effects of enemy exploitation of the electro-magnetic spectrum. As a nation, the US is dependent upon both offensive and defensive information operations in order to attain information superiority. As a component of a coalition, regardless of the size of participation, the defensive weaknesses of a single member could form the weakness of a coalition. We must enable our coalition partners with defensive information operations capabilities that will limit an adversary's ability to influence coalition operations.

TRANSFORMATION

At present, although the Army is capable of full spectrum dominance, its organization and force structure are not optimized for strategic responsiveness. Army options available to warfighting CINCs for joint contingency response are too limited.⁴² The Army's transformation is

intended to enable forces to use the most modern equipment, training, and capabilities to get to the locations where it is needed most, in the least amount of time, with the most firepower and self protection possible.

The Transformation Campaign Plan charts our course to transform The Army into an Objective Force, while maintaining our non-negotiable contract to fight and win our Nation's wars -- being trained and ready at all times as we execute operational requirements in support of National Military Strategy and CINC requirements.⁴³ This campaign plan allows for the maintenance and upgrade of legacy forces, while initial and subsequent interim capabilities are designed and fielded. As initial and interim capabilities are being built, the objective force will be tailored using the best capabilities available from the interim and initial designs, as well as the most advanced technologies available at the time.

Command and control capabilities for US forces will advance as expeditiously as possible, as the transformation takes the Army from the legacy force to the Objective force. The advancements in the world of telecommunications are frankly moving much faster than those of the Army Transformation, and there is no slow down in sight. If the command and control capabilities of the transformed Army are to be as effective as the weapons systems that they are envisioned to support, there must be a concerted effort to expedite the procurement of leading edge telecommunications technologies that will be imbedded in the interim and objective force structures.

The certainty that future US operations will include allies can be matched with the need to share different C2 information with those same allies. Without interoperability between forces, the exchange of C2 information will be limited, hampering the speed and precision that our forces will need. The changing complexities of international diplomacy, and evolutions in alliances will determine who the US will be involved with in multi-national operations of the future. While historically strong allies can usually be counted upon to remain strong allies, it is likely that the US will see more nations looking for cooperative military relations and alliances, in search of stability, friendship, and support. The expansion of our involvement with these nations will have to take into consideration the extent to which we feel comfortable sharing our national information with them. Such assessments will have to be made on a continuous basis, with the most frequent reviews being done for nations we have most recently chosen to trust, and ongoing reviews for those that we have trusted in the past.

As we transform the Army, we must design the command and control of our forces to be as responsive as the technology and pace of operations that we may engage in. The decision-

making process must become rapid, or units will find themselves waiting for instructions and commanders will lose opportunities to exploit enemy vulnerabilities.

Technology will continue to evolve and unforeseen capabilities will emerge. The US Army's anticipation of future capabilities being available when they are needed, while acknowledging that the same future capabilities have yet to be designed, is testimony to our trust that technology will continue to advance. Under the Army's transformation, capabilities that are available off the shelf are being integrated into the Initial and Interim Brigade Combat Teams. The Initial Brigade Combat Team (IBCT) Organizational and Operational (O&O) concept is clear in our needs for strategically responsive and dominant capability in preparation for full spectrum operations where the likely operational environment will includes coalition involvement. (Although) the Interim Brigade Combat Team operates under division or corps command, the ... environment will often require it to maintain direct links with multinational forces.⁴⁴

Looking even further into the future, Army planners anticipate even greater opportunities for advancements in communications technology for the objective force. The communications designs for the objective force are components of the Warfighter Information Network – Tactical (WIN-T). The WIN-T Operational Requirements Document is open-ended in respect to technology.

WIN-T will be a bandwidth and spectrum-efficient, Joint Technical Architecture (JTA)-compliant, commercial standards-based network capability that is easy to upgrade, operate, maintain, manage, and train. WIN-T's overall design and acquisition strategy must enable fielding of new technologies as they become available. The objective is to routinely place state-of-the-art technologies and their enabling capabilities into the hands of the warfighters. WIN-T is comprised of network infrastructure (integrated switching, routing, and transmission systems), network management, network services, Information Assurance (IA), and user interfaces that provide voice, video, and data services throughout the battlespace. 45

The multinational interoperability functions of WIN-T in the Operational Requirement Document are described as being designed to "support rapid deployment with Joint and multinational interoperability in mind." This description leaves a great deal of room for interpretation regarding the differences in capabilities that are to be available with the initial fielding of WIN-T (threshold time frame) and what capabilities can be delayed until the objective time frame. This can be most clearly seen in the ambiguity between allied and coalition networks. The ORD states under the category of "Interoperability: The network must

interoperate with service-specific, Joint, U.S. commercial networks, allied, European commercial, coalition, and non-DoD networks."

There is little time to sort through the requirements for coalition interoperability, even with the long-term view expressed in the Transformation Strategy. While definitions of allied and coalition have yet to be detailed in the WIN-T ORD, the IBCT plans appear to be taking shape and initial procurement plans are already forming up with the selection of some vehicle and weapons systems having been completed already.

Army Transformation details for the next five years are fairly clear. Those for the following five years are more general. Things in 2015 and beyond – the time for which Army Transformation is ultimately geared – are distant glimmers toward which the plan is continually inching. As the time is projected forward, the more nebulous the plan becomes simply because many of the key elements remain to be invented.⁴⁸

As the glimmer of the Objective combat force is brought into focus, the communications design for the threshold requirements for WIN-T are uncertain. The Army must embrace a method to achieve coalition command and control interoperability and begin building toward it now, so that it can be put into place with the Objective force, if not sooner.

Reliable communications is the most important piece of the battle-command system able to realize the full potential of future organizations.⁴⁹ We must keep pace with rapidly evolving information technology so that we can cultivate and harvest the promise of information superiority among U.S. forces and coalition partners.⁵⁰ Now is the time to review the future capabilities that the Army will need and ensure that information exchange with allied partners is not only possible, but also probable.

Regional CINCs often look for assistance and cooperation from nations within their geographic areas of responsibility. Interoperability serves to improve the means of communications between the US and these nations. It is useful to examine the value of international relations and interoperability in a CINC's region.

US PACIFIC COMMAND (PACOM) EXPERIENCES

US PACOM serves as one example of US international diplomacy. With forces dispersed across the largest geographic area of responsibility of any of the regional CINCs, PACOM has geographic responsibility for more than 50 percent of the earth's surface, where nearly 60 percent of the world's population lives. Within this region, four of the world's six largest armed forces reside, and most importantly US PACOM represents the US Armed Forces participation in five of the seven worldwide mutual defense treaties. In this diverse multinational

environment, coalition command and control interoperability is one of the key elements of PACOM's theater engagement planning.

PACOM's push for more open, more inclusive relationships with military forces throughout its area of operations has become a new catalyst for change throughout the region. In concert with carefully considered political support from the US, PACOM's military activities in the Asia-Pacific complement regional activities aimed at bolstering the spirit of trust and cooperation that is gradually taking hold throughout the region.⁵¹

US PACOM found during operations in East Timor that each participating country had its own unique operational procedures. These created difficulties at the operation's 'seams' - points where forces from different countries had a high degree of operational interaction. ⁵² In order to work through some of these challenges, PACOM will explore international "standardized procedures" this spring in exercise "Team Challenge 2001." This combined exercise will link several formerly bilateral exercises into a multilateral training operation. Exercises like these enable nations with diverse capabilities to come together and learn from each other. Overseas presence enhances coalition operations by promoting joint and combined training and encouraging responsibility sharing on the part of friends and allies. ⁵³

RECOMMENDATIONS

Seamless command and control in a multi-national environment has been, and continues to be an objective requirement for US forces. The current National Military Strategy states that ... a secure Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) architecture must be designed and developed from the outset for rapid deployment and with joint and multinational interoperability in mind. Because we will often act in concert with likeminded nations, as we implement JV 2010, we must also retain interoperability with our allies and potential coalition partners. This vision of future capabilities guides our warfighting requirements and procurement, and focuses technological development. JV2010's key enablers of information superiority and technological innovation will transform the current concepts of maneuver, strike, protection, and logistics into the new operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection.

Using some of our unsurpassed capabilities in the pursuit of common interests and values demonstrates leadership and encourages confidence and greater contributions by others, reducing the demand on ourselves in the long run.⁵⁶ Just as we should be prepared to act as a single nation, we should also be looking forward to the resultant benefits of the use of our

evolutionary technologies. The investments made in technology by the US, should result in improvements in coalition interoperability, which would encourage wider participation by other nations in multinational operations, and correspondingly decrease the overall operational tempo of US forces.

Our international exercise program is one activity that fosters greater interoperability with coalition partners. Exercises enhance interoperability and readiness and demonstrate our ability to form and lead effective coalitions. They demonstrate our capabilities and resolve to friends and potential adversaries alike. They provide realistic conditions for working with the technologies, systems, and operational procedures that will be crucial in times of crisis. Exercises encourage burden sharing on the part of friends and allies, and facilitate regional integration. Exercises such as the Joint Warrior Interoperability Demonstrations and the Simulation and C2 Information Systems Connectivity Experiments should be funded to look beyond existing problems and toward evolving systems, such as those being developed for the Army Transformation, that will benefit the most from coalition interoperability.

POLICY

The limitations that cause for the differentiation between what information is releasable to allies, and what is not, creates an enormous obstacle for interoperability. Separate networks must be established for data that is not releasable and what is. Two actions should be taken to rectify this problem.

First, the standards that determine what is releasable to foreign governments should be reviewed. The policy and standards that apply to SECRET information should be reversed to enable more open disclosure rather than more comprehensive non-disclosure that exists today. According to DOD 5200.1-H, the Handbook for Writing Security Classification Guidance, the application of precise classification guidance is prerequisite to effective and efficient information security and assures that security resources are expended to protect only that which truly warrants protection in the interests of national security. So Only the most sensitive information which can not be shared with allies should be marked NO FOREIGN DISSEMINATION (NOFORN). If this were the case then Non-releasable SECRET information should be the exception rather than the rule.

Second, the networks that carry the information should be class marked to carry the most common traffic, rather than the traffic that is most highly classified. If the majority of the traffic were to be SECRET, which was releasable, then the standard networks should be class marked as such, rather than the SECRET NOFORN that exists today.

Each of these recommendations has direct applicability to the improvement of coalition interoperability for the Interim and Objective Forces. If the majority of the data carried were releasable rather than restricted, the standard would be to disclose rather than withhold. There would also be significantly fewer requirements for gateways and firewalls between networks since the allies would now be able to connect directly to the Tactical Internet that will carry the majority of the data to the Interim Brigade Combat Team.

TECHNOLOGY

The standardization of how we use the technologies that are evolving can have a profound effect on the simplicity, or the difficulty, involved to enable coalition interoperability. Under the most recently revised DOD 5000 acquisition process, the conditions have been set to ensure that future procurements such as those under the Army Transformation conform to the appropriate standards. Interoperability requirements must be identified as Key Performance Parameters (KPP) and must be demonstrated prior to production. ⁵⁹

Two potential shortfalls still exist though. First, the drafting of the interoperability KPPs for the program being procured have to be appropriate and specific enough to ensure that the required performance is actually what is delivered. As stated earlier, the KPPs for the WIN-T program are not defined as clearly as they need to be. Second, the new acquisition process refers to interoperability in a very general sense. The interoperability it promotes is not aligned with either US joint Services interoperability or international interoperability. As advancements are made with technologies, we have to consider the applications for the technologies that are being developed and the means that are used to acquire them in order to produce interoperable solutions.

STRATEGIC VISION

The uncertain future is here today. We are deceiving ourselves if we think that we have 15 years to prepare for an opposition that understands our center of gravity and is already skilled in the use of information technologies and/or the delivery of asymmetric warfare.

Developers should search out increasingly effective capabilities that will empower our forces of the future. These capabilities must include coalition interoperability as a required performance parameter, and not just as a catchy phrase. Organizations and doctrine should be created now to meet the demands that we may face tomorrow using the capabilities that we possess today or expect to possess in the future. We must take up the challenge of modernizing our organizations and doctrine today, with the innovations we have at hand and

achieve success, despite the uncertainties and limited appreciation for what the next decade may have in store for us.

The future of the Army rests on our ability to depict the requirements of the future before the time comes to employ them. Coalition partnerships are necessary today, and will be necessary in the future. The Army Transformation will jumpstart the process by investing in today's off-the-shelf technology to stimulate the development of doctrine, organizational design, and leader training even as we begin a search for new technologies for the objective force. The Army must look upon the requirement to interoperate with allies in the future in the same way.

CONCLUSION

The transformation will transition the entire Army into a force that is strategically responsive and dominant at every point on the spectrum of operations. The aggressive pursuit of the most advance technologies available is admirable and undeniably necessary. Our challenge is to determine how to best leverage new, advancing information technologies to provide warfighters the most effective means to achieve information superiority, not only with our sister services, but with our coalition partners and allies. Knowledge dominance is the key to success for the transformation of the Army.

The risks of failure, due to a lack of multi-national Command and Control interoperability, are growing with each international operation US forces undertake. On any given day in 1997, the Total (U.S.) Force was deployed in support of 10 Joint/Combined Operations and participates in 11 exercises in over 70 countries. The post-1997 QDR force has experienced an even higher operational tempo. The potential for operational failure, in peace operations or in war, due to the challenges of international interoperability, exist. We must accept the fact that such risks will grow if the US does not match our needs for information superiority and technological innovation with the increasingly multinational composition of future deployments. The IBCT will have no more communications interoperability than the legacy forces that it replaced if immediate steps are not taken to embrace the policy and technical obstructions that have hampered command and control in the past, and will put it at risk in the future.

WORD COUNT = 8799

ENDNOTES

- ¹ William J. Clinton, <u>1997 State of the Union Address</u>, Remarks by the President in State of the Union Address, 105th Cong., 4 February 1997, (Washington D.C: U.S. Congress), 11.
 - ² Joint Chiefs of Staff, Joint Vision 2020, June 2000, 12.
 - ³ Joint Chiefs of Staff, Joint Vision 2020, June 2000, 2.
- ⁴ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 21.
 - ⁵ Joint Chiefs of Staff, Joint Vision 2020, June 2000, 6.
- ⁶ William J. Clinton, <u>A National Security Strategy for a New Century</u> (Washington, D.C.: The White House, October 1998), 11.
- ⁷ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 2.
- ⁸ Joint Chiefs of Staff, <u>Doctrine for Joint Operations</u>, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), xvi.
- ⁹ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 8.
- ¹⁰ William J. Clinton, <u>A National Security Strategy for a New Century</u> (Washington, D.C.: The White House, October 1998), 10.
- ¹¹ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 10.
- ¹² William J. Clinton, <u>A National Security Strategy for a New Century</u> (Washington, D.C.: The White House, October 1998), 16.
- ¹³ Joint Chiefs of Staff, <u>Doctrine for Joint Operations</u>, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), II-15.
- ¹⁴ Joint Chiefs of Staff, <u>Doctrine for Joint Operations</u>, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), II-15.
- ¹⁵ Joint Chiefs of Staff, <u>Doctrine for Joint Operations</u>, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), I-6.
- ¹⁶ Joint Chiefs of Staff, <u>Joint Doctrine for Multinational Operations</u>, Joint Publication 3-16 (Washington, D.C.: U.S. Department of Defense, 5 April 2000), II-7.
- ¹⁷ William J. Clinton, <u>A National Security Strategy for a New Century</u> (Washington, D.C.: The White House, October 1998), 18.

- ¹⁸ Joint Chiefs of Staff, <u>Doctrine for Joint Operations</u>, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), I-6.
- ¹⁹ David S. Alberts and Richard E. Hayes, <u>Command Arrangements for Peace Operations</u> (Washington, D.C.: U.S. Government Printing Office, 1995), 9.
- ²⁰ Joint Chiefs of Staff, <u>Doctrine for Joint Operations</u>, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), II-7.
- ²¹ David S. Alberts and Richard E. Hayes, <u>Command Arrangements for Peace Operations</u> (Washington, D.C.: U.S. Government Printing Office, 1995), 10.
- ²² Joint Chiefs of Staff, <u>Doctrine for Joint Operations</u>, Joint Publication 3-0 (Washington, D.C.: U.S. Department of Defense, 1 February 1995), II-8.
- ²³ Joint Chiefs of Staff, <u>Joint Doctrine for Information Operations</u>, Joint Publication 3-13 (Washington, D.C.: U.S. Department of Defense, 9 October 1998), I-9.
- ²⁴ Joint Chiefs of Staff, <u>Joint Doctrine for Information Operations</u>, Joint Publication 3-13 (Washington, D.C.: U.S. Department of Defense, 9 October 1998), I-5.
- ²⁵ "The Global English Newsletter," 5th Edition, 1999; available from http://www.english.co.uk/newsletter/gens/gen5.shtml. Internet. Accessed 16 March 2001.
- ²⁶ John G. Roos, "More Inclusive Partnerships," <u>Armed Forces Journal International</u> (February 2001): 39.
- ²⁷ John G. Roos, "More Inclusive Partnerships," <u>Armed Forces Journal International</u> (February 2001): 30.
 - ²⁸ Joint Chiefs of Staff, Joint Vision 2020, June 2000, 15.
- ²⁹ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 4.
- ³⁰ William J. Clinton, <u>A National Security Strategy for a New Century</u> (Washington, D.C.: The White House, October 1998), 21.
- Joint Chiefs of Staff, <u>Department of Defense Dictionary of Military and Associated Terms</u>, Joint Publication 1-02 (Washington, D.C.: U.S. Department of Defense, 1 February 1995).
 - ³² Joint Chiefs of Staff, Joint Vision 2020, June 2000, 15.
- ³³ Joint Chiefs of Staff, <u>Joint Doctrine for Multinational Operations</u>, Joint Publication 3-16 (Washington, D.C.: U.S. Department of Defense, 5 April 2000), III-13.
- ³⁴ Defense Information Systems Agency, <u>Defense Message System Product Plan</u>, version 3.03 (Washington D.C.: U.S. Department of Defense, 20 August 1999), 19.

- ³⁵ Defense Information Systems Agency, <u>Defense Message System Product Plan</u>, version 3.03 (Washington D.C.: U.S. Department of Defense, 20 August 1999), 18.
- ³⁶ Defense Information Systems Agency, <u>Defense Message System Product Plan</u>, version 3.03 (Washington D.C.: U.S. Department of Defense, 20 August 1999), 32.
- ³⁷ Defense Information Systems Agency, <u>Defense Message System Product Plan</u>, version 3.03 (Washington D.C.: U.S. Department of Defense, 20 August 1999), 6.
- ³⁸ Joint Chiefs of Staff, <u>Joint Doctrine for Multinational Operations</u>, Joint Publication 3-16 (Washington, D.C.: U.S. Department of Defense, 5 April 2000), III-9.
- ³⁹ Robert Forrester <robert.forrester@GD-CS.com>, "BATTLE COMMAND BATTLE LABORATROY BE-WEEKLY FDIC REPORT," electronic mail message to William Pope <william.pope@carlisle.army.mil>, 16 March 2001.
- ⁴⁰ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 18.
- ⁴¹ Joint Chiefs of Staff, <u>Joint Doctrine for Multinational Operations</u>, Joint Publication 3-16 (Washington, D.C.: U.S. Department of Defense, 5 April 2000), III-16.
- ⁴² Department of the Army, <u>Initial Brigade Combat Team (IBCT) Operational and Organizational (O&O) Concept</u>, Version 4 (Washington, D.C.: U.S. Department of the Army, 18 April 2000), 4.
- ⁴³ Department of the Army, <u>Army Transformation</u> briefing, (Washington, D.C.: U.S. Department of the Army, 17 October 2000), 4.
- ⁴⁴ Department of the Army, <u>Initial Brigade Combat Team (IBCT) Operational and Organizational (O&O) Concept</u>, Version 4 (Washington, D.C.: U.S. Department of the Army, 18 April 2000), 18.
- ⁴⁵ Department of the Army, <u>Warfighter Information Network Tactical (WIN-T) Operational Requirements Document (ORD)</u>, Version 5 (Washington, D.C.: U.S. Department of the Army, 13 November 2000), 3.
- ⁴⁶ Department of the Army, <u>Warfighter Information Network Tactical (WIN-T) Operational Requirements Document (ORD)</u>, Version 5 (Washington, D.C.: U.S. Department of the Army, 13 November 2000, 2.
- ⁴⁷ Department of the Army, <u>Warfighter Information Network Tactical (WIN-T) Operational Requirements Document (ORD)</u>, Version 5 (Washington, D.C.: U.S. Department of the Army, 13 November 2000, 10.
- ⁴⁸ Dennis Steele, "The Army Magazine Hooah Guide to Army Transformation," <u>Army Magazine</u> Vol. 51 No. 2 (February 2001): 23.

- ⁴⁹ Huba Wass de Czege and Jacob D. Biever, "Six Compelling Ideas On the Road to a Future Army," <u>Army Magazine</u> Vol. 51 No. 2 (February 2001): 46.
- ⁵⁰ William J. Clinton, <u>A National Security Strategy for a New Century</u> (Washington, D.C.: The White House, October 1998), 12.
- ⁵¹ John G. Roos, "More Inclusive Partnerships," <u>Armed Forces Journal International</u> (February 2001): 39.
- ⁵² John G. Roos, "More Inclusive Partnerships," <u>Armed Forces Journal International</u> (February 2001): 30.
- ⁵³ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 19.
- ⁵⁴ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 29.
- ⁵⁵ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 17.
- ⁵⁶ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 16.
- ⁵⁷ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 13.
- ⁵⁸ Department of Defense, <u>The Handbook for Writing Security Classification Guidance</u>, DoD 5200.1-H, (Washington, D.C.: U.S. Department of Defense, 13 December 1996), 6.
- ⁵⁹ Kristine A. DiMarco, "The New DoD Systems Acquisition Process," briefing slides with scripted commentary, Washington D.C., Department of Defense, 10 February 2001.
- ⁶⁰ Department of the Army, "The Army Vision," February 2000; available from http://www.army.mil/armyvision/armyvis.htm; Internet; accessed 30 March 2001.
- ⁶¹ Department of the Army, "The Army Vision," February 2000; available from http://www.army.mil/armyvision/armyvis.htm; Internet; accessed 30 March 2001.
- ⁶² John P. Cavanaugh, "Transformation: a cultural revolution across the Army," <u>Army Communicator</u> Vol. 25 No. 4 (Winter 2000): 6.
- ⁶³ John M. Shalikashvili, <u>National Military Strategy of the United States of America</u>, (Washington, D.C.: The Joint Chiefs of Staff, 1997), 13.
- ⁶⁴ Henry H. Shelton, "A Word from the Chairman," <u>Joint Force Quarterly</u>, no. 25 (Summer 2000): 4.

BIBLIOGRAPHY

- Alberts, David S., and Richard E. Hayes. <u>Command Arrangements for Peace Operations</u>. Washington, D.C.: U.S. Government Printing Office, 1995.
- Cavanaugh, John P. "Transformation: a cultural revolution across the Army." <u>Army Communicator</u> Vol. 25 No. 4 (Winter 2000): 6.
- Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, October 1998.
- Clinton, William J. <u>1997 State of the Union Address</u>. Remarks by the President in State of the Union Address. 105th Cong., 4 February 1997. Washington D.C.: U.S. Capitol.
- Defense Information Systems Agency. <u>Defense Message System Product Plan</u>. Version 3.03. Washington D.C.: U.S. Department of Defense. 20 August 1999.
- Department of the Army. <u>Army Transformation</u> briefing. Washington, D.C.: U.S. Department of the Army, 17 October 2000.
- Department of the Army, "The Army Vision," February 2000; available from http://www.army.mil/armyvision/armyvis.htm; Internet; accessed 30 March 2001.
- Department of the Army. <u>Initial Brigade Combat Team (IBCT) Operational and Organizational (O&O) Concept</u>. Version 4. Washington, D.C.: U.S. Department of the Army. 18 April 2000.
- Department of the Army. Warfighter Information Network Tactical (WIN-T) Operational Requirements Document (ORD). Version 5. Washington, D.C.: U.S. Department of the Army. 13 November 2000.
- Department of Defense. <u>The Handbook for Writing Security Classification Guidance</u>. DoD 5200.1-H. Washington, D.C.: U.S. Department of Defense. 13 December 1996.
- Department of Defense. <u>Information Security Program</u>. DoD 5200.1-R. Washington D.C.: U.S. Department of Defense. 17 January 1997.
- DiMarco, Kristine A. "The New DoD Systems Acquisition Process." Briefing slides with scripted commentary. Washington D.C.: Department of Defense. 10 February 2001.
- Forrester, Robert <robert.forrester@GD-CS.com>. "BATTLE COMMAND BATTLE LABORATROY BE-WEEKLY FDIC REPORT." Electronic mail message to William Pope <william.pope@carlisle.army.mil>. 16 March 2001.
- "The Global English Newsletter." 5th Edition, 1999. Available from http://www.english.co.uk/newsletter/gens/gen5.shtml. Internet. Accessed 16 March 2001.
- Roos, John G., "More Inclusive Partnerships." <u>Armed Forces Journal International</u> (February 2001): 39.

- Shalikashvili, John M. National Military Strategy of the United States of America. Washington, D.C.: The Joint Chiefs of Staff, 1997.
- Shelton, Henry H. "A Word from the Chairman." <u>Joint Force Quarterly</u>. no. 25 (Summer 2000): 4.
- Steele, Dennis. "The Army Magazine Hooah Guide to Army Transformation." <u>Army Magazine</u> Vol. 51 No. 2 (February 2001): 23.
- U.S. Joint Chiefs of Staff, <u>Joint Vision 2020</u>, Washington, D.C.: U.S. Government Printing Office, June 2000.
- U.S. Joint Chiefs of Staff. <u>Department of Defense Dictionary of Military and Associated Terms</u>. Joint Publication 1-02. Washington, D.C.: U.S. Department of Defense, 1 February 1995.
- U.S. Joint Chiefs of Staff. <u>Doctrine for Joint Operations</u>. Joint Publication 3-0. Washington, D.C.: U.S. Department of Defense, 1 February 1995.
- U.S. Joint Chiefs of Staff, <u>Joint Doctrine for Information Operations</u>, Joint Publication 3-13. Washington, D.C.: U.S. Department of Defense, 9 October 1998.
- U.S. Joint Chiefs of Staff. <u>Joint Doctrine for Multinational Operations</u>. Joint Publication 3-16. Washington, D.C.: U.S. Department of Defense, 5 April 2000.
- Wass de Czege, Huba, and Jacob D. Biever. "Six Compelling Ideas On the Road to a Future Army." <u>Army Magazine</u> Vol. 51 No. 2 (February 2001): 46.